UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,448	04/27/2001	Gregory Neil Houston	05456.105005	9082

69151 7590 05/18/2010

KING & SPALDING, LLP
INTELLECTUAL PROPERTY DEPT. - PATENTS
1180 PEACHTREE STREET, N.E.
ATLANTA, GA 30309-3521

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2435	
MAIL DATE	**DELIVERY MODE**
05/18/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/844,448	**Applicant(s)** HOUSTON ET AL.	
	Examiner Ponnoreay Pich	**Art Unit** 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 April 2010*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4,6,49 and 60-75* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4,6,49 and 60-75* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114 was filed in this application after a decision by the Board of Patent Appeals and Interferences, but before the filing of a Notice of Appeal to the Court of Appeals for the Federal Circuit or the commencement of a civil action. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 4/19/10 has been entered.

Claims 1, 4, 6, 49, and 60-75 are pending. Applicant's amendments were fully considered. Applicant's arguments directed at the amended claims were fully considered, but are moot in view of new rejections made below in response to the amendments.

Oath/Declaration

The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

> The oath or declaration is defective because the oath submitted on 9/24/01 identifies all the inventors as the sole or first inventor. It is unclear who should be listed as the first inventor and it is further unclear if all the people signing their respective copies of the oath understand that they are not the sole inventor of the invention being claimed.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 49 and 62-70 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

1. As per claims 49 and 66, the claims are directed towards a computer program product comprising a computer-readable storage medium having computer-readable program code embodied therewith. However, the specification as originally filed failed to set forth the metes and bounds of what is meant to be encompassed by the term "computer-readable storage medium". As such, it would have been reasonable to interpret the term as encompassing signals per se having stored thereon or encoded with computer readable program code. As per In *re Nuijten, 500 F.3d 1346, 1357 (Fed. Cir. 2007)*, such a claim is not statutory.
2. Claims 62-65 and 67-70 are also not statutory because they are also directed towards signals per se.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 4, 6, 49, and 60-75 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hill et al (US 6,088,804) in view of Harrow et al (US 5,375,199).

Claims 1 and 66:

As per claim 1, Hill discloses:

1. A plurality of security devices (i.e. security agents) generating security event data comprising a plurality of alerts in response to detecting a security event in a distributed computing environment, the security devices being logically coupled to a computer having a display (Fig 1; col 4, lines 11-17 and 30-41; and col 5, lines 7-15).
2. Configuring an event data report that identifies a portion of the security event data as result data (Fig 5; Fig 7; and col 7, lines 46-63). *Note that not all event types must be mapped, the system can be configured to respond only to specific types of attacks, and that the process shown in Figure 5 is initiated by an administrator. This implies the administrator being able to configure which event data are reported.*
3. The computer receiving a selection of one or more user-configurable variables operable for filtering the security event data (col 7, lines 46-63), the user configurable variables comprising at least one of a location of a security event, a source of security event, and a destination of the security event (col 6, lines 1-8 and Fig 7).
4. The computer collecting the security event data generated by the plurality of security devices (col 4, lines 30-41; col 5, lines 7-15; and col 8, lines 12-21).

5. The computer storing the collected security event data (col 8, lines 29-34).
6. The computer filtering the collected security event data using the one or more user-configurable variables to produce the result data for the event data report (col 4, lines 30-41; col 7, lines 46-63; Fig 6; and Fig 7).
7. The computer transmitting the result data to one or more clients (col 4, lines 53-61).
8. The one or more clients displaying the event data report comprising the result data (Co 5, lines 7-15; and Fig 7).

Hill does not explicitly disclose <u>the computer presenting a user interface via the display</u> for configuring the event data report and the computer receiving the selection <u>via the user interface</u>. However, as discussed above already, the particular attacks mapped and responded to by Hill's invention is configurable (i.e. by a user). Some method which allows the user to make selections to thereby configure the event data report must be utilized by Hill's invention. Harrow discloses a system in which a computer presents a user interface via a display for configuring which activities to monitor and the computer receiving the selection via the user interface 9col 7, lines 27-54).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Hill's invention to such that the configuring of the event data report was done by the computer presenting a user interface via the display and the computer receiving a selection via the user interface of computer user-configurable variables. One skilled would have been motivated to do so because use of a GUI display for the user to configure Hill's system would reduce the learning curve for training new users on Hill's monitoring system. Further, as discussed above, Hill's system already uses some form of interface for allowing the use to configure his system, thus incorporating Harrow's teachings within Hill's invention is nothing more simple substitution of one known element (i.e. configuration scheme) for another to achieve predictable results (i.e. configuration via a GUI display).

Claim 66 is directed towards a program product used to implement the method of claim 1 and is rejected for similar reasons.

Claims 49 and 71:

As per claim 49, Hill discloses:

1. A plurality of security devices (i.e. security agents) generating security event data comprising a plurality of alerts in response to detecting a security event in a distributed computing environment, the security event data comprising a plurality of alerts (Fig 1; col 4, lines 11-17 and 30-41; and col 5, lines 2-15).
2. The security device sending the security event data to a computer coupled to a display (col 4, lines 30-41; col 5, lines 2-6; col 7, lines 7-15; and col 8, lines 12-21).
3. The computer transferring the security event data for storage in a database (col 5, lines 2-6 and 39-57 and Fig 6).
4. Configuring an event data report that identifies a portion of the security event data as result data (Fig 5; Fig 7; and col 7, lines 46-63). *Note that not all event*

types must be mapped, the system can be configured to respond only to specific types of attacks, and that the process shown in Figure 5 is initiated by an administrator. This implies the administrator being able to configure which event data are reported.

5. The computer receiving a selection of one or more user-configurable variables operable for filtering the security event data (col 7, lines 46-63), the user configurable variables comprising at least one of a security event type, a priority of a security event, and an identification of a system that detected a security event (col 6, lines 1-8; Fig 6; and Fig 7).
6. The computer filtering the stored security event data using the one or more user-configurable variables to produce the result data for the event data report (col 4, lines 30-41).
7. The computer displaying via the display the event data report and the result data comprising filtered alerts based on the user-configurable/selected variables (Fig 7).

Hill does not explicitly disclose the computer presenting a user interface via the display for configuring the event data report and the computer receiving the selection via the user interface. However, as discussed above already, the particular attacks mapped and responded to by Hill's invention is configurable (i.e. by a user). Some method which allows the user to make selections to thereby configure the event data report must be utilized by Hill's invention. Harrow discloses a system in which a computer presents a user interface via a display for configuring which activities to monitor and the computer receiving the selection via the user interface 9col 7, lines 27-54).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Hill's invention to such that the configuring of the event data report was done by the computer presenting a user interface via the display and the computer receiving a selection via the user interface of computer user-configurable variables. One skilled would have been motivated to do so because use of a GUI display for the user to configure Hill's system would reduce the learning curve for training new users on Hill's monitoring system. Further, as discussed above, Hill's system already uses some form of interface for allowing the use to configure his system, thus incorporating Harrow's teachings within Hill's invention is nothing more simple substitution of one known element (i.e. configuration scheme) for another to achieve predictable results (i.e. configuration via a GUI display).

Claim 71 is directed towards a program product used to implement the method of claim 49 and is rejected for similar reasons.

Claim 4:

Hill further discloses wherein collecting the security event data comprises:

1. A sensor generating security event data (col 4, lines 30-40).
2. The sensor sending the security event data to a collector coupled to the computer (col 4, lines 53-60).

3. The computer converting the event data to a common format (col 5, lines 7-8 and 34-37).

Claims 6, 68, 63, and 73:

As per claim 6, Hill further discloses the computer searching the stored security event data for additional information identifying a security event (col 8, lines 40-49).

Claims 68, 63, and 73 are rejected for similar reasons as claim 6.

Claims 60, 69, 62, and 74:

As per claim 60, Hill further discloses the step of the security devices pre-filtering the security event data prior to transmitting the pre-filtered security event data to the computer (col 4, lines 30-46; col 8, lines 12-21; and Fig 5, step 88).

Claims 69, 62, and 74 are rejected for similar reasons as claim 60.

Claims 61, 70, 64, and 75:

As per claim 61, Hill further discloses the step of performing an analysis on the collected security event data, the analysis comprising at least one of (a) comparing a source address of a first detected security vent data with a source address of a second detected security event and (b) comparing information associated with each detected security event with information identifying a known vulnerability of the distributed computing environment (col 8, lines 35-49).

Claims 70, 64, and 75 are rejected for similar reasons as claim 61.

Claims 67, 65, and 72:

Hill further discloses computer-readable program code to convert the event data to a common format (col 5, lines 7-8 and 34-37).

Claims 65 and 72 are rejected for similar reasons as claim 67.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is (571) 272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ponnoreay Pich/
Primary Examiner, Art Unit 2435